Protect yourself from paying a double excess

Cyber assisted fraud on law practices, leading to the loss of client funds, has increased substantially over the past 5 years and the sophistication of this fraudulent activity has evolved over time.

Fraudulent payment redirections are perpetrated as a result of cyber criminals penetrating a practice's computer systems and sending fraudulent emails masquerading as a solicitor. Sometimes the fraudulent emails originate outside the law practice, and solicitors (or their staff) are duped into paying client funds to cyber criminals.

Since 2017, when Lawcover received its first cyber fraud claim from a law practice, we have taken significant steps to warn and to help law practices guard against these attacks. Our specific cyber fraud program of resources for law practices includes cyber incident crisis assistance through Lawcover's group cyber risk policy, which we purchase each year and provide to all law practices at no cost when they renew their professional indemnity policy with us. We also provide risk management seminars, online modules, webinars, podcasts and other risk mitigation education on this issue.

Despite these comprehensive steps to help raise awareness and provide law practices with assistance to potentially avoid cyber attacks, some law practices are submitting substantial claims to Lawcover and it has become quickly evident that they have not put in place minimal, if any security measures or processes, to guard against payment direction fraud. It is for this reason that Lawcover has included a double excess in the Lawcover 2022/23 PII policy wording.

From 1 July 2022 a double excess will be payable by law practices for:

> ***claims*** *arising from any payment or electronic funds transfer made in response to a purported instruction or authorisation, which the law practice did not take reasonable steps to verify*

Reasonable risk management steps – verify bank details

All law practices should have in place a "read out, read back" policy to verify bank account details. Prior to client funds being transferred, staff should verify bank account details by contacting the client and reading out the bank details then having the client read back the details. It's important that process takes place using a phone number obtained from a source other than the email containing the bank details.

Cyber criminals will actively try to dissuade law practices from verifying bank details by phone or will send alternate phone numbers to be contacted on for verification. Staff should be wary about any communication which offers alternate phone numbers or tries to steer away from face to face or telephone contact.

Warn your clients

At the beginning of a matter, wherever possible take a range of phone contact details (office, mobile, landline) and preferably bank account details as well. Include these on the physical file and use them as a source of truth.

Warn clients about the risk of cyber criminals, and the steps you are taking to combat that risk. Inform clients that you will never change your trust account details by email. While a warning in an email footer is useful, cyber criminals have intercepted these communications and deleted the footer before sending a fake email.

Ask clients to contact the law practice by phone to verify trust account details before transferring money into trust. Ask them to check phone details via the law practice website to avoid cyber criminals providing false verification by phone.

This is an all-staff problem

Unlike other professional indemnity issues, mistakes leading to payment redirection fraud can arise from mistakes of any staff member. Have all your staff complete our complimentary online cyber security training course "Cyber claims in legal practice" which contains useful examples of the types of attacks experienced by a legal practice and what you can do to manage the risk. Available on the Risk Online eLearning platform - Register for the course.

Elissa Baxter
Chief Legal Officer